Document Number: NN47240-400
August 2008
Phone 1-800-4Nortel
http://www.nortel.com

Release Notes for Nortel Threat Protection System Release 4.7.0.7

NORTEL

August 28, 2008

Contents

Introduction

Release 4.7.0.7 of the Nortel Threat Protection System resolves a security issue that can occur in very rare circumstances on Defense Centers that manage sensors with RNA detection engines. This security issue does not affect the Intrusion Sensor.

Nortel strongly recommends that you install this patch as soon as possible. If you cannot install this patch on all your Defense Centers in a timely manner, contact Support for information about how to mitigate your risk.

These release notes are valid for Release 4.7.0.7 of Nortel Defense Centers.

These release notes describe:

Product Compatibility

Release 4.7.0.7 of the Defense Center can manage:

- versions 4.7.0.x of the Intrusion Sensor
- version 4.6.x.x of the Intrusion Sensor
- version 4.0.0.x of the RNA Sensor (also called the RTI Sensor)

Features and Functionality

Release 4.7.0.7 does not contain any new features or functionality.

Issues Resolved in Release 4.7.0.7

The following issues are resolved in Release 4.7.0.7:

- Resolved a security-related issue that in rare cases could cause a Defense Center that manages sensors with RNA to become unavailable or to allow remote code execution on the Defense Center. (44352)

Updating Existing Defense Centers

The following sections help you prepare for and install Release 4.7.0.7 on your existing Defense Centers. Do not install this patch on Intrusion Sensors.

NOTE – For information about installing and configuring new appliances, see the installation guide on the Documentation CD that was delivered with your appliance.

Planning for the Update

This section outlines how to plan for the update of your Defense Center and any sensors that it manages.

1 Make sure your appliances are running the correct version.

To update to Release 4.7.0.7, your appliances must be running at least Release 4.7.

If you are running an earlier version, you can obtain updates from the Nortel Support Site.

2 Make sure you have enough free disk space and allow enough time for the update.

For appliances with up to 10 million events, the update takes approximately 15 minutes, so you should plan to perform the update during non-peak hours. This patch requires approximately 35MB on the `/` partition and 330MB on the `/var` partition.

3 Optionally, back up your event and configuration data.

Although the update process retains event and configuration data, Nortel strongly recommends that you back the data up to a local computer before you perform the update. See your user guide for information about backing up your appliance.

4 Perform the update, as described in Updating the Defense Center (page 7).

In general, you can monitor its progress in the Defense Center's task queue (**Operations > Monitoring > Task Status**).

IMPORTANT! When you upgrade a Defense Center that is half of a high availability pair, the Defense Centers in the pair stop sharing configuration information until the second Defense Center is upgraded. You must upgrade both Defense Centers separately.

5 Complete any required post-update steps, as described in After You Update Your Appliances (page 8).

Nortel recommends that you check the Support Site for the latest SEU and vulnerability database (VDB) update.

Updating the Defense Center

To update the Defense Center:

1 Download the Nortel Threat Protection System Release 4.7.0.7 update script (*Nortel_TPS_Defense_Center_Patch_4.7.0_to_4.7.0.7-1117.sh*) from the Nortel Support Site.

IMPORTANT! Download files directly from the Support Site and do not transfer them by email. If you transfer an update file by email, it may become corrupted.

2 Select **Operations > Update**.

The Patch Management Update page appears.

3 Click **Upload Update** to browse to the location where you saved the update script, then click **Upload**.

The update appears in the Updates list.

4 Next to the update you just uploaded, click **Install**.

The Install Update page appears.

5 Under Selected Update, select the Defense Center and click **Install**.

6 Confirm that you want to install the update and reboot the Defense Center.

The update is installed and the Defense Center reboots. You can monitor the update's progress in the task queue (**Operations > Monitoring > Task Status**).

Warning: Do not use the web interface to perform any other tasks until the update has completed and the Defense Center reboots. Note that before the update completes, the Nortel Threat Protection System may log you out. If this occurs, log in to the appliance and view the task queue. If the update is still running, continue to refrain from using the web interface until the update has completed. If the task queue stops updating with current status, manually refresh your browser. If you encounter issues with the update, for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress, do not restart the update. Instead, please contact Support.

7 After the update finishes, and the Defense Center reboots, log into the Nortel Threat Protection System.

8 Clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

9 Select **Operations > Help > About** and confirm that the software version is listed as Release 4.7.0.7.

10 Verify that all managed sensors are successfully communicating with the Defense Center.

11 Continue with the tasks you need to perform after the update.

For more information, see After You Update Your Appliances (page 8).

After You Update Your Appliances

After you complete the update, you must:

- Install any patches or updates to the Nortel Threat Protection System that are available on the Support Site
- Install the latest SEU and reapply intrusion policies to any IPS detection engines

IMPORTANT! Applying an intrusion policy causes IPS detection engines to restart, which can cause a short pause in processing and, for most detection engines with inline interface sets, may cause a few packets to pass through the sensor uninspected.

- Install the latest vulnerability database (VDB), then push and install the VDB update on any managed Intrusion Sensor with RNA

For more information, refer to the Nortel Threat Protection System User Guide.

Uninstalling the Update

Uninstalling the update results in an appliance running Release 4.7.0.5. For information on uninstalling Release 4.7.0.5, refer to the release notes for that version.

To uninstall Release 4.7.0.7:

1. Select **Operations > Update**.

   The Patch Management Update page appears.

2. Next to the uninstaller that matches the update you want to remove, click **Install**.

   On the Defense Center, the Install Update page appears. Under Selected Update, select the Defense Center and click Install.

   On the Intrusion Sensor, there is no intervening page.

3. The Install Update page appears. Under Selected Update, select the Defense Center and click **Install**.
4. Confirm that you want to uninstall the update and reboot the appliance.

   The update is removed, the appliance reboots and returns to Release 4.7.0.5. You can monitor the uninstallation progress in the task queue (**Operations > Monitoring > Task Status**).

Warning: If the task queue stops updating with current status, manually refresh your browser. If you encounter issues with the uninstallation, for example, if the task queue indicates that the uninstallation has failed or if a manual refresh of the task queue shows no progress, do not restart the uninstallation. Instead, please contact Support.

5. After the uninstall finishes and the appliance reboots, log into the web interface once again.
6. Select **Operations > Help > About** and confirm that the software version is listed as Release 4.7.0.5.

Known Issues

There are no new known issues with this release. However, be sure to review the known issues in the release notes for previous releases.

How to get help

This section explains how to get help for Nortel products and services.

Finding the latest updates on the Nortel web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software, click one of the following links:

Link to	Takes you directly to the:
Latest software	Nortel page for software located at www.nortel.com
Latest documentation	Nortel page for documentation located at www.nortel.com

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

- www.nortel.com/support

If you have any questions or require assistance with the Nortel Defense Center or Intrusion sensors (Intrusion Sensor, RNA Sensor, or any of the software sensors), contact Nortel Support.

- Visit the Nortel Support Site.
- Email Nortel Support at support@nortel.com.

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Nortel Threat Protection System Release Notes
Nortel Threat Protection System

Release: 4.7.0.7
Document Number: NN47240-400
Part Code: 320740-I
Document status: Standard
Document Version: Version 03.01
Document release date: August 2008

To provide feedback, or to report a problem in this document, go to www.nortel.com/documentfeedback.

NORTEL